Installation Guide
Revision 1.0

VirusScan® Enterprise

version 8.0*i*

McAfee® SECURITY

COPYRIGHT

Copyright © 2004 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, ClickNet, CNX, CNX Certification Certified Network Expert and design, Covert, Design (Stylized E), Design (Stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Entercept, Enterprise SecureCast, Enterprise SecureCast (in Katakana), ePolicy Orchestrator, EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, IntruVert Networks, LANGuru, LANGuru (in Katakana), M and Design, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, Network Associates Coliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, Recoverkey, Recoverkey - International, Registry Wizard, RingFence, Router PM, SecureCast, SecureSelect, Sniffer, Sniffer (in Hangul), SpamKiller, Stalker, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, WinGauge, Your E-Business Defender, Zip Manager are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Sniffer® brand products are made only by Network Associates, Inc. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

♦ Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). ♦ Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. ♦ Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that Network Associates provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. ♦ Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software written by Douglas W. Sauder. ♦ Software developed by the Apache Software Foundation (http://www.apache.org/). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. ♦ Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. ♦ Software copyrighted by Expat maintainers. ♦ Software copyrighted by The Regents of the University of California, © 1989. ♦ Software copyrighted by Gunnar Ritter. ♦ Software copyrighted by Sun Microsystems®, Inc.© 2003. ♦ Software copyrighted by Gisle Aas. © 1995-2003. ♦ Software copyrighted by Michael A. Chase, © 1999-2000. ♦ Software copyrighted by Neil Winton, © 1995-1996. ♦ Software copyrighted by RSA Data Security, Inc., © 1990-1992. ♦ Software copyrighted by Sean M. Burke, © 1999, 2000. ♦ Software copyrighted by Martijn Koster, © 1995. ♦ Software copyrighted by Brad Appleton, © 1996-1999. ♦ Software copyrighted by Michael G. Schwern, © 2001. ♦ Software copyrighted by Graham Barr, © 1998. ♦ Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. ♦ Software copyrighted by Frodo Looijaard, © 1997. ♦ Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. ♦ Software copyrighted by Beman Dawes, © 1994-1999, 2002. ♦ Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software copyrighted by Simone Bordet & Marco Cravero, © 2002. ♦ Software copyrighted by Stephen Purcell, © 2001. ♦ Software developed by the Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software copyrighted by International Business Machines Corporation and others, © 1995-2003. ♦ Software developed by the University of California, Berkeley and its contributors. ♦ Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/). ♦ Software copyrighted by Kevlin Henney, © 2000-2002. ♦ Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. ♦ Software copyrighted by David Abrahams, © 2001, 2002. See http://www.boost.org/libs/bind/bind.html for documentation. ♦ Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software copyrighted by Boost.org, © 1999-2002. ♦ Software copyrighted by Nicolai M. Josuttis, © 1999. ♦ Software copyrighted by Jeremy Siek, © 1999-2001. ♦ Software copyrighted by Daryle Walker, © 2001. ♦ Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. ♦ Software copyrighted by Samuel Krempp, © 2001. See http://www.boost.org for updates, documentation, and revision history. ♦ Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software copyrighted by Cadenza New Zealand Ltd., © 2000. ♦ Software copyrighted by Jens Maurer, © 2000, 2001. ♦ Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software copyrighted by Ronald Garcia, © 2002. ♦ Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. ♦ Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software copyrighted by Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software copyrighted by Paul Moore, © 1999. ♦ Software copyrighted by Dr. John Maddock, © 1998-2002. ♦ Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. ♦ Software copyrighted by Peter Dimov, © 2001, 2002. ♦ Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. ♦ Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

PATENT INFORMATION

Protected by US Patents 6,006,035; 6,029,256; 6,035,423; 6,151,643; 6,230,288; 6,266,811; 6,269,456; 6,457,076; 6,496,875; 6,542,943; 6,594,686; 6,611,925; 6,622,150.

Contents

1 Introducing VirusScan Enterprise 5

Before you begin installation 5
Pre-installation recommendations 6
System requirements 8
Deployment, updating, and management options 9
Pre-configuring the installation package 9
McAfee AutoUpdate Architect and McAfee Installation Designer 10
ePolicy Orchestrator 10
Installation and configuration for use with other products 11
Netopsystems' FEAD® Optimizer© 12
Windows Terminal Server 12
EMC Celerra™ server 12
Check Point™ 12
Product license 13
Using this guide 13
Audience 13
Conventions 14
Resources 15
Getting product information 15
Contact information 16

2 Installing the Software 17

Installing VirusScan Enterprise 17
Using the Setup utility to install program files 18
Choosing a typical or custom installation 22
Typical installation 23
Custom installation 25
Using the command line to install program files 33
Command-line syntax 34
Installation scenarios 34
Logging installation progress 36
Installation properties 37

Selecting features 40
Setting restart options 41
Using a login script to install program files 41
Incompatible software removed 42
Files installed 44
VirusScan folder 44
Resources folder 45
Engine folder 45
Testing your installation 46

3 Modifying or Repairing the Software 47

Modifying installed features 48
Using the Setup utility to modify features 48
Using the command line to modify program features 52
Reinstalling or repairing program files 53
Using the Setup utility to reinstall or repair program files 53
Reinstalling program files 55
Repairing program files 57
Using the command line to reinstall or repair the program files 59

4 Removing the Software 61

Using the Setup utility to remove the product 62
Using the command line to remove the product 65
Using the Add/Remove Programs utility to remove the product 66

A Configuring Netopsystems' FEAD Optimizer 67

Optimized file defaults 67
Command-line properties and switches 68

Index 69

Introducing VirusScan Enterprise 1

This guide introduces McAfee® VirusScan® Enterprise software version 8.0*i* and provides information about installing, modifying, and removing the software.

These topics are included in this section:

- *Before you begin installation*.
- *Using this guide* on page 13.
- *Resources* on page 15.

Before you begin installation

Before you start the installation, we recommend that you review these topics to ensure that you are prepared:

- *Pre-installation recommendations* on page 6.
- *System requirements* on page 8.
- *Deployment, updating, and management options* on page 9.
- *Pre-configuring the installation package* on page 9.
- *Installation and configuration for use with other products* on page 11.
- *Product license* on page 13.

Pre-installation recommendations

Complete these items before you begin the installation process:

Product software

Locate the VirusScan Enterprise software. McAfee Security distributes VirusScan Enterprise software in two ways:

1. On a product CD.
2. If you do not have a product CD, you can download the program files from the McAfee Security web site:
   a. Create a temporary folder on your hard drive.
   b. Download the archive file from the McAfee Security download web site. See *Contact information* on page 16 for information about accessing the web site.
   c. Use a decompression utility, such as WinZip, to extract the files you downloaded to the temporary folder.

Readme

Locate and read the *Readme* file to identify special installation instructions or issues. You can find it in the same location as the product software.

Installation rights

Verify that you have local administrator rights for the computer on which you plan to install VirusScan Enterprise.

Preserve settings

When upgrading from an earlier version of the software, decide whether you want to preserve settings.

If you are installing VirusScan Enterprise on a computer with an earlier version of VirusScan, VirusScan Enterprise, or NetShield, you have the option of preserving the settings from the earlier version.

- These settings are preserved:
  - Configuration settings for saved tasks.
  - User-specified extensions.
  - Exclusions settings.
  - Virus definition (DAT) file version, if the previous version is later than the version in the installation package.
  - Scanning engine version, if the previous version is later than the version in the installation package.
  - Log file names and locations are preserved.

    NOTE
    Although the name and location are preserved, the log file format is changed from ANSI to UTF8. When the format is changed, the log file is renamed to *.BAK.

- The registry keys containing installation file locations and product versions are not preserved:

If you do not want to preserve settings, you can either install the software and deselect the option to preserve setting, or you can remove the previous version of the software first, then install VirusScan Enterprise.

System requirements

Verify that your server and/or workstation meet these system requirements before you start the installation process.

- **Processor** — An Intel processor or compatible architecture. McAfee Security recommends an Intel Pentium or Celeron processor running at a minimum of 166MHz.
- **Operating system** — Any of these Microsoft Windows platforms:

Server	Workstation
Windows NT Server 4.0, with Service Pack 6 or 6a.	Windows NT Workstation 4.0, with Service Pack 6 or 6a.
Windows NT Enterprise Server 4.0, with Service Pack 6 or 6a.	Windows 2000 Professional, with Service Pack 2, 3, or 4.
Windows NT Terminal Server Edition, with Service Pack 6.	Windows XP Home and Professional, with Service Pack 1.
Windows Server 2003 Standard.	Windows XP Tablet PC.
Windows Server 2003 Enterprise.	
Windows 2000 Server, with Service Pack 3 or 4.	
Windows 2000 Advanced Server, with Service Pack 3 or 4.	
Windows NT Server 4.0, with Service Pack 6 or 6a.	

- **Browser** — Microsoft Internet Explorer, version 5.0 or later.
- **Memory** — 32MB RAM minimum. For information on optimal operating system performance, review the Microsoft guidelines for minimum RAM configuration.
- **Free disk space** — Adequate hard disk space.
  - **38MB** — A complete installation of all the program's features and components occupies approximately 38MB of disk space on your computer.
  - **22MB** — The installation process uses an additional 22MB of temporary disk space, which is freed when the installation is complete.
  - **40MB** — If you are using a management tool to deploy VirusScan Enterprise, you must have an additional 40MB of disk space available to deploy the installation package. This disk space is normally freed when the installation is complete, depending on the management tool you are using.
- **Other** — A CD-ROM drive or an Internet connection.

Deployment, updating, and management options

Decide how you plan to deploy, manage, and update the product. If you use supporting tools to deploy, pre-configure, update, or manage VirusScan Enterprise, the installation procedure may vary.

Pre-configuring the installation package

To pre-configure the VirusScan Enterprise installation package, we recommend that it includes:

- Where and how you get updates.
- When you check for updates (the default is daily at 17:00 local time to the computer).
- Which policy settings should be defined.

Use either of these methods to pre-configure the installation package:

- *McAfee AutoUpdate Architect and McAfee Installation Designer* on page 10.
- *ePolicy Orchestrator* on page 10.

McAfee AutoUpdate Architect and McAfee Installation Designer

Use McAfee AutoUpdate Architect and McAfee Installation Designer to pre-configure the installation package.

> **NOTE**
> If you plan to use the McAfee Security HTTP or FTP update sites as your update location, skip Step 1 and Step 2. The VirusScan Enterprise software comes pre-configured to get updates from these locations. The HTTP site is the default location and the FTP site is configured as the next location in the repository list.
>
> For more information about updating or using the McAfee Security HTTP or FTP update sites, see the *VirusScan Enterprise Product Guide*.

1. Install McAfee AutoUpdate Architect and use it to configure the VirusScan Enterprise repository list, SITELIST.XML. The repository list contains the available updating sites that VirusScan Enterprise uses for updating. See the *McAfee AutoUpdate Architect Product Guide* for more information.
2. Export the repository list, SITELIST.XML, to a temporary folder.
3. Install McAfee Installation Designer and use it to customize the installation options for VirusScan Enterprise. See the *McAfee Installation Designer Product Guide* for more information.

ePolicy Orchestrator

If you installed ePolicy Orchestrator prior to deploying VirusScan Enterprise, you can use it to pre-define the policy settings and update configuration.

ePolicy Orchestrator version 3.0 or later can be used to create and manage your update repositories. This ensures that product installations and updates are applied from a local source.

We recommend that before you push the software to client computers via ePolicy Orchestrator, you first use McAfee Installation Designer to replace or update the default virus definition (DAT) and engine files included in the installation package. This ensures that the client computer has the most current protection at installation time and also saves network bandwidth by not having to retrieve the updated files after installation.

Installation and configuration for use with other products

If you are installing VirusScan Enterprise software where third-party products are installed, or plan to use the VirusScan Enterprise software with supporting products, you may be required to vary the installation procedure or perform additional configuration.

These topics are included in this section:

- *Netopsystems' FEAD® Optimizer©* on page 12.
- *Windows Terminal Server* on page 12.
- *EMC Celerra™ server* on page 12.
- *Check Point™* on page 12.

Netopsystems' FEAD® Optimizer©

The VirusScan Enterprise installation file (.MSI) has been optimized using the Netopsystems' Fast Electronic Application Distribution (FEAD® Optimizer©) technology. This significantly reduces the size of the installation file until it is recomposed. The installation file is recomposed at different times depending on which installation method you use:

- **Setup utility**. The installation file is automatically recomposed before the installation begins.
- **Command line**. You can apply special command-line properties and switches to recompose the installation files. See *Configuring Netopsystems' FEAD Optimizer* on page 59 for more information.
- **McAfee Installation Designer**. Use this program to recompose the installation file, then optimize it again after changes have been made. See the *McAfee Installation Designer Product Guide* for more information.

Windows Terminal Server

If Windows NT Terminal Server Edition or Windows 2000 or 2003 Terminal Server Application is installed, and the Setup utility is used to install the VirusScan Enterprise software, the installation stops and the user is notified that they must install the product using the Add/Remove Programs utility that is included in the Windows Control Panel.

> **NOTE**
> This installation method is not required if you are using ePolicy Orchestrator to deploy the VirusScan Enterprise software.

EMC Celerra™ server

If you are installing the VirusScan Enterprise software to an EMC Celerra server, you must first install the EMC Scanner Server software, then install the VirusScan Enterprise software. This ensures that the VirusScan Enterprise software configures correctly with the EMC Celerra server settings.

Check Point™

The VirusScan Enterprise software integrates with Check Point™ VPN-1/FireWall-1® SCV. This integration allows you to prevent clients without up-to-date anti-virus protection from accessing the corporate network through the Virtual Private Network (VPN). See the *McAfee Trusted Connection Implementation Guide* for configuration information.

Product license

If you are installing the product for the first time, the product is licensed during the installation process. Skip this section and go to *Installing VirusScan Enterprise* on page 17.

If you are installing a licensed version of the VirusScan Enterprise software over an evaluation version, you must upgrade the evaluation version to a licensed version. The license does not automatically upgrade itself from an evaluation version.

> **WARNING**
> You must perform the license upgrade before the evaluation period expires. If you do not, the scanning and updating functions stop until you replace the evaluation version with a licensed version of the product.

Use one of these methods to upgrade an evaluation version of VirusScan Enterprise to a licensed version:

- McAfee Installation Designer upgrades an installed evaluation version to a licensed version:
  - Install the licensed version of VirusScan Enterprise.
  - Use McAfee Installation Designer to upgrade the license. Refer to the *McAfee Installation Designer Product Guide* for specific details.
- Remove the evaluation version of the product and install the licensed version of the product. Note that you lose all of the settings from the previous installation. This method is only recommended if you cannot use McAfee Installation Designer to upgrade the license.

Using this guide

When using this guide, consider the following:

- *Audience*.
- *Conventions* on page 14.

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's anti-virus and security program.
- Users who are responsible for updating virus definition (DAT) files on their workstation, or configuring the software's detection options.

Conventions

This guide uses the following conventions:

Bold

All words from the user interface, including options, menus, buttons, and dialog box names.

Example

Type the **User name** and **Password** of the desired account.

`Courier`

The path of a folder or program; a web address (URL); text that represents something the user types exactly (for example, a command at the system prompt).

Examples

The default location for the program is:

```
C:\Program Files\Network Associates\VirusScan
```

Visit the Network Associates web site at:

```
http://www.networkassociates.com
```

Run this command on the client computer:

```
C:\SETUP.EXE
```

Italic

For emphasis or when introducing a new term; for names of product manuals and topics (headings) within the manuals.

Example

Refer to the *VirusScan Enterprise Product Guide* for more information.

<TERM>

Angle brackets enclose a generic term.

Example

In the console tree under **ePolicy Orchestrator**, right-click <SERVER>.

NOTE

Supplemental information; for example, an alternate method of executing the same command.

WARNING

Important advice to protect a user, computer system, enterprise, software installation, or data.

Resources

Refer to these sections for additional resources:

- *Getting product information*.
- *Contact information* on page 16.

Getting product information

Installation Guide *†	System requirements and instructions for installing and starting the software.
Product Guide *	Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures. *VirusScan Enterprise Product Guide* *Alert Manager™ Product Guide* *Desktop Firewall Product Guide* *ePolicy Orchestrator® Product Guide* *McAfee AutoUpdate Architect™ Product Guide* *McAfee Installation Designer™ Product Guide*
Help §	High-level and detailed information on configuring and using the software. *What's This?* field-level help.
Configuration Guide *	*For use with ePolicy Orchestrator.* Procedures for configuring, deploying, and managing your McAfee Security product through ePolicy Orchestrator management software.
Implementation Guide *	Supplemental information for product features, tools, and components. *McAfee Trusted Connection Implementation Guide*
Release Notes ‡	*ReadMe.* Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.
Contacts ‡	Contact information for McAfee Security and Network Associates services and resources: technical support, customer service, AVERT (Anti-Virus Emergency Response Team), beta program, and training. This file also includes phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world.

* An Adobe Acrobat .PDF file on the product CD or the McAfee Security download site.

† A printed manual that accompanies the product CD. Note: Some language manuals may be available only as a .PDF file.

‡ Text files included with the software application and on the product CD.

§ Help accessed from the software application: Help menu and/or Help button for page-level help; right-click option for *What's This?* help.

Contact information

Technical Support	
Home Page	http://www.networkassociates.com/us/support/
KnowledgeBase Search	https://knowledgemap.nai.com/phpclient/homepage.aspx
PrimeSupport Service Portal *	http://mysupport.nai.com
McAfee Security Beta Program	http://www.networkassociates.com/us/downloads/beta/
Security Headquarters — AVERT (Anti-Virus Emergency Response Team)	
Home Page	http://www.networkassociates.com/us/security/home.asp
Virus Information Library	http://vil.nai.com
Submit a Sample — AVERT WebImmune	http://vil.nai.com/vil/submit-sample.asp
AVERT DAT Notification Service	http://vil.nai.com/vil/join-DAT-list.asp
Download Site	
Home Page	http://www.networkassociates.com/us/downloads/
DAT File and Engine Updates	http://www.networkassociates.com/us/downloads/updates/
	ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
Product Upgrades *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp
Training	
McAfee Security University	http://www.networkassociates.com/us/services/education/mcafee/university.htm
Network Associates Customer Service	
E-mail	services_corporate_division@nai.com
Web	http://www.nai.com/us/index.asp
	http://www.networkassociates.com/us/support/default.asp
US, Canada, and Latin America toll-free:	
Phone	**+1-888-VIRUS NO** or **+1-888-847-8766**
	Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting Network Associates and McAfee Security— including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

* Logon credentials required.

Installing the Software 2

This version of the VirusScan Enterprise software replaces earlier versions of VirusScan, VirusScan Enterprise, NetShield, and NetShield for Celerra™ version 4.5 for Celerra™ filers. It installs on both workstations and servers.

These topics are included:

- *Installing VirusScan Enterprise*.
- *Incompatible software removed* on page 42.
- *Files installed* on page 44.
- *Testing your installation* on page 46.

Installing VirusScan Enterprise

Use any of these methods to install VirusScan Enterprise:

- *Using the Setup utility to install program files* on page 18.
- *Using the command line to install program files* on page 33.
- *Using a login script to install program files* on page 41.

Using the Setup utility to install program files

Review the *System requirements* on page 8 before you begin the installation process.

1 Start the Setup utility using one of these methods.

- From the product CD:
  - a Insert the CD into the CD-ROM drive.
  - b Click **Install** from the **Welcome** dialog box.
- From the command line:
  - a Click **Start**, then select **Run**.
  - b Type `<X>:\SETUP.EXE` in the **Run** dialog box, then click **OK**.

    Here, `<X>:` represents the drive letter for your CD-ROM, or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click **Browse**. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.
- From the installation folder:
  - a Browse to the location where you installed the program files.
  - b Double-click SETUP.EXE.

The **Netopsystems' FEAD Optimizer** dialog box appears.

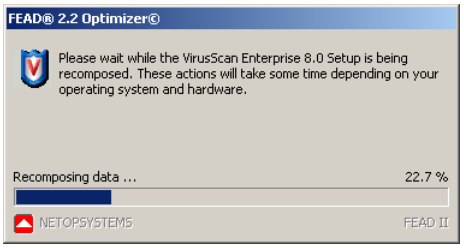
FEAD® 2.2 Optimizer©
Please wait while the VirusScan Enterprise 8.0 Setup is being recomposed. These actions will take some time depending on your operating system and hardware.
Recomposing data ...
22.7 %
NETOPSYSTEMS
FEAD II

Figure 2-1. Netopsystems' FEAD Optimizer

NOTE
It may take a few minutes to recompose the files. The amount of time it takes depends on your operating system and hardware. The next dialog box appears when the files have been recomposed.

The **McAfee VirusScan Enterprise Setup** dialog box appears.

McAfee VirusScan Enterprise Setup
McAfee VirusScan Enterprise Setup
This setup wizard will install McAfee VirusScan Enterprise to your server or workstation. Before continuing, please review the following product information.
McAfee® Security VirusScan® Enterprise
Version 8.0
Copyright © 2004 Networks Associates Technology, Inc. All Rights Reserved.
Thank you for using VirusScan Enterprise software. For a description of product features, an overview of product system requirements, and known issues for this release, see the README.TXT file that is included with the software on the CD you received, or that is available as a separate download from the McAfee Security web site.
McAfee Security strongly recommends that you review the contents of the
View Readme
Next >
Cancel

Figure 2-2. McAfee VirusScan Enterprise Setup

2 Click **View Readme** to display the release notes for this product. When finished, close the README file, then click **Next**.

The **Network Associates Licensing** dialog box appears.

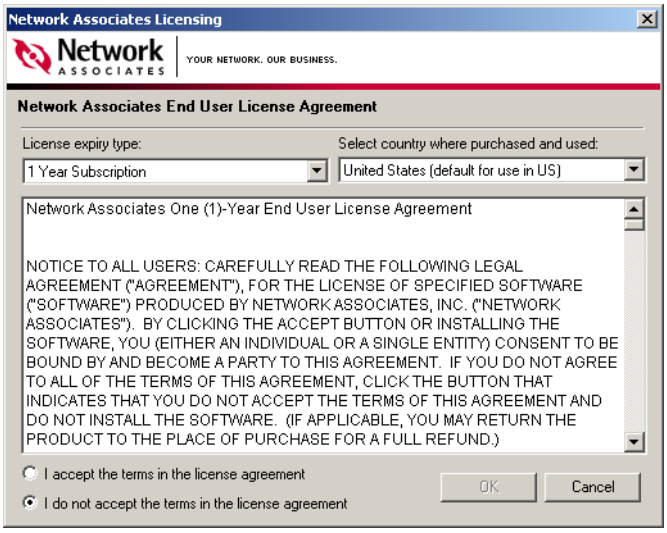
Network Associates Licensing
Network
ASSOCIATES
YOUR NETWORK. OUR BUSINESS.
Network Associates End User License Agreement
License expiry type:
1 Year Subscription
Select country where purchased and used:
United States (default for use in US)
Network Associates One (1)-Year End User License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY NETWORK ASSOCIATES, INC. ("NETWORK ASSOCIATES"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)
I accept the terms in the license agreement
I do not accept the terms in the license agreement
OK
Cancel

Figure 2-3. Network Associates Licensing

3 In the **License expiry type** text box, click ▼ to select the type of license.

> **NOTE**
> The license type must match the type of license that you purchased. If you are unsure of which type of license to select, contact the person from whom you purchased the software.

4 In the **Select country where purchased and used** text box, click ▼ to select the country in which you are using the software.

5 Read the license agreement carefully, then choose one of these options:

- If you *agree* to the license terms, select **I accept the terms in the license agreement**, then click **OK** to continue.
- If you *do not agree* to the terms, select **I do not accept the terms in the license agreement**, then click **Cancel** to stop the installation process.

6 At this point, the procedure varies depending on whether you are installing the software for the first time or upgrading from a previous version. Choose the method that applies to your installation:

First-time installation

If you are installing the VirusScan Enterprise software for the first time, or reinstalling the software (Setup does not detect a previously installed version of VirusScan, VirusScan Enterprise, or NetShield), the **Select Setup Type** dialog box appears. Go to *Choosing a typical or custom installation* on page 22 to continue.

Installing over a previous version

If you are installing VirusScan Enterprise software over NetShield, VirusScan, or an earlier version of VirusScan Enterprise, the **Previous Version Detected** dialog box appears.

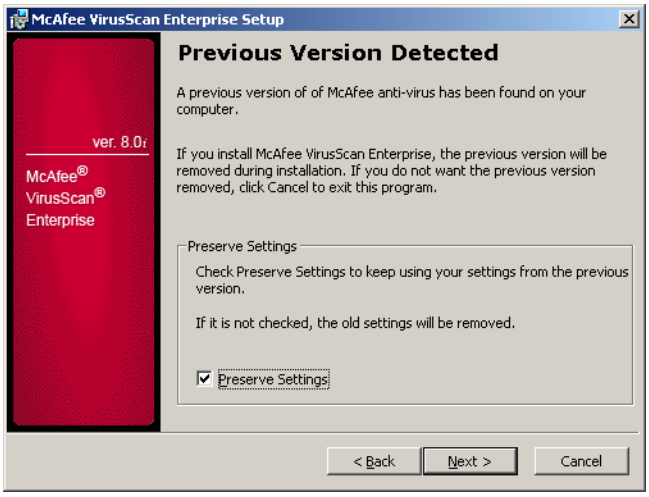
McAfee VirusScan Enterprise Setup
Previous Version Detected
A previous version of of McAfee anti-virus has been found on your computer.
If you install McAfee VirusScan Enterprise, the previous version will be removed during installation. If you do not want the previous version removed, click Cancel to exit this program.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Preserve Settings
Check Preserve Settings to keep using your settings from the previous version.
If it is not checked, the old settings will be removed.
Preserve Settings
< Back
Next >
Cancel

Figure 2-4. Previous Version Detected

7 **Preserve Settings** *(Default)*. To use the settings from the previously installed version of the software, click **Next**.

> **NOTE**
> See *Preserve settings* on page 7 for a list of settings that are preserved and lost.

The **Select Setup Type** dialog box appears. Go to *Choosing a typical or custom installation* on page 22 to continue.

Choosing a typical or custom installation

You must have completed the steps in *Using the Setup utility to install program files* on page 18 to begin a typical or custom installation.

In the **Select Setup Type** dialog box, decide which installation type you want to use:

McAfee VirusScan Enterprise Setup
Select Setup Type
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Typical
Installs the full set of features that includes VirusScan Console, On-Access Scanner, E-mail Scanner, On-Demand Scanner, AutoUpdate, Buffer Overflow Protection, and Command Line Scanner. If you are installing to a server, Alert Manager can also be installed.
Custom
Installs a selected set of features that includes a partial set or all of the features included in a Typical installation. You can also use the custom option to install Alert Manager to a workstation.
Install To
C:\Program Files\Network Associates\VirusScan\
Browse...
Disk Space
< Back
Next >
Cancel

Figure 2-5. Setup Type

- **Typical.** Installs the software with all utilities.

  McAfee Security recommends this installation type for most environments.

  > **NOTE**
  > **Typical** installation does not give you the capability of importing the AutoUpdate repository list or setting a user interface password. You must select **Custom** installation to use these features.

  Go to *Typical installation* on page 23 to begin the typical installation process.

- **Custom**. Installs all or selected features, Alert Manager and Desktop Firewall if they not already installed and gives you the options to import the AutoUpdate repository list and specify user interface security settings.

  Go to *Custom installation* on page 25 to begin the custom installation process.

Typical installation

You must have completed the steps in *Using the Setup utility to install program files on page 18* before you can begin the typical installation process.

1 In the **Select Setup Type** dialog box, select the installation type and where to install it:

   a Select **Typical**.

   b Under **Install To**, accept the default path, type a new path, or click **Browse** to locate to a path.

   By default, Setup installs the VirusScan Enterprise program files to this path:

   ```
   <drive>:\Program Files\Network Associates\VirusScan\
   ```

   c Click **Disk Space** to view the disk space requirements, then click **OK** to return to the **Select Setup Type** dialog box.

2 Click **Next** to display the **Ready to install** dialog box.

3 If you are satisfied with all of the installation settings you selected, click **Install** to begin the installation process.

   NOTE
   To review or change any of the settings, click **Back**, then return to the **Ready to install** dialog box and click **Install.**

   The **Installing McAfee VirusScan Enterprise** dialog box shows the status of the installation.

4 In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to run an update task and/or an on-demand scan task upon completion of installation.

McAfee VirusScan Enterprise Setup
ver. 8.0i
McAfee®
VirusScan®
Enterprise
McAfee VirusScan Enterprise setup has completed successfully.
Allows you to update your virus definition (DAT) files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.
Update Now
Automatically checks for updates of virus defintion (DAT) files and/or scan engine and downloads any available updates.
Run On-Demand Scan
Examines all fixed drives for infected files. Infections are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\.
Finish
Cancel

Figure 2-6. Setup completed successfully — update and scan options

- **Update Now** *(Default).* When selected, an update task is automatically performed upon completion of installation.
- **Run On-Demand Scan** *(Default).* When selected, an on-demand scan task is automatically performed upon completion of installation.

5 Click **Finish**.

NOTE
Depending on the options you selected in Step 4, the program may run the update program or an on-demand scan at this time. If you selected both options, the update task runs first, then the on-demand scan task runs.

6 You are prompted to restart your computer to load the network driver.

McAfee VirusScan Enterprise Setup
The network driver is installed but you must restart the computer in order to load it.
Port Blocking, Infection Trace, and Infection Trace Blocking are disabled until the computer is restarted.
OK

Figure 2-7. Load network driver

WARNING
You must restart the computer to load the network driver. Loading this network driver enables the Port Blocking, Infection Trace, and Infection Trace Blocking features in VirusScan Enterprise.

Click **OK**, then restart the computer.

7 You may be prompted to restart your computer again when the installation process completes. If so, the **VirusScan Enterprise Setup** dialog box appears. You can choose to restart at this time or at a later time.

Custom installation

You must have completed the steps in *Using the Setup utility to install program files* on page 18 before you can begin the custom installation.

1 In the **Select Setup Type** dialog box, select the type and installation path:

   a Select **Custom**.

   b Under **Install To**, accept the default installation path or click **Browse** to locate a path.

   By default, Setup installs the VirusScan Enterprise program files to this path:

   ```
   <drive>:\Program Files\Network Associates\VirusScan\
   ```

   c Click **Disk Space** to view the disk space requirements, then click **OK** to return to the **McAfee VirusScan Enterprise Setup** dialog box.

2 Click **Next** to continue.

3 In the **Feature Selection** dialog box, select which features you want to install and where you want to install them.

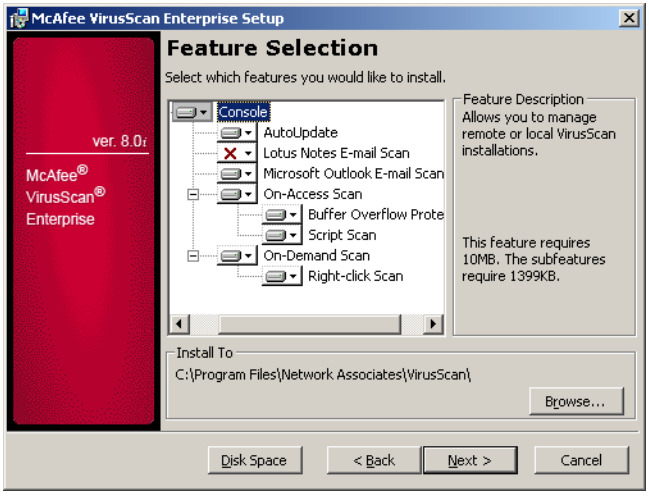

Figure 2-8. Feature Selection

a Under **Select which features you would like to install**, these features are available for selection:

- **Console** (Default)
- **AutoUpdate**
- **Lotus Notes E-mail Scan**
- **Microsoft Outlook E-mail Scan**
- **On-Access Scan**

  Buffer Overflow Protection

  NOTE
  This feature cannot be installed on 64-bit systems or if either the Entercept agent or the Cisco Security agent are found on the local computer.

  Script Scan

  NOTE
  This feature cannot be installed on 64-bit systems.

- **On-Demand Scan**

  Right-click Scan

  NOTE
  This feature cannot be installed on 64-bit systems.

b For each selected feature, you can also select a corresponding action from the drop-down menu. Click next to the selected feature, to display the action menu, then select the action for that feature.

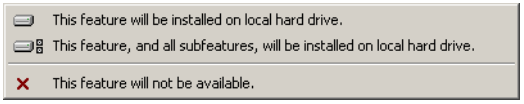
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Figure 2-9. Feature action options

c Under **Install To**, accept the default path, type a new path, or click **Browse** to select a path.

4 Click **Next** to continue.

5 In the **Install McAfee Products** dialog box, choose whether you want to install Alert Manager and/or Desktop Firewall after the VirusScan Enterprise installation completes:

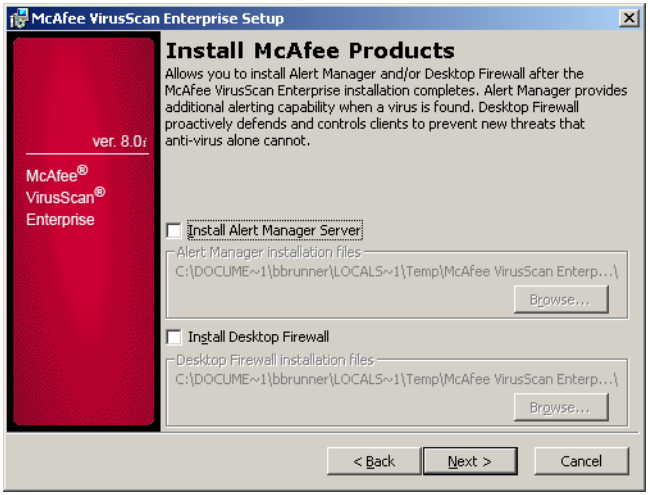
McAfee VirusScan Enterprise Setup
Install McAfee Products
Allows you to install Alert Manager and/or Desktop Firewall after the McAfee VirusScan Enterprise installation completes. Alert Manager provides additional alerting capability when a virus is found. Desktop Firewall proactively defends and controls clients to prevent new threats that anti-virus alone cannot.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Install Alert Manager Server
Alert Manager installation files
C:\DOCUME~1\bbrunner\LOCALS~1\Temp\McAfee VirusScan Enterp...\
Browse...
Install Desktop Firewall
Desktop Firewall installation files
C:\DOCUME~1\bbrunner\LOCALS~1\Temp\McAfee VirusScan Enterp...\
Browse...
< Back
Next >
Cancel

Figure 2-10. Install McAfee Products

- **Install Alert Manager Server**. Installs the Alert Manager product found in the location shown under **Alert Manager installation files**.

  Alert Manager installation files. Accept the default path or click **Browse** to select the location where Alert Manager is installed.

- **Install Desktop Firewall**. Installs the Desktop Firewall product found in the location shown under **Desktop Firewall installation files**.

  Desktop Firewall installation files. Accept the default path or click **Browse** to select the location where Desktop Firewall is installed.

  WARNING
  If you do not install Alert Manager and/or Desktop Firewall as part of a custom installation the first time you install VirusScan Enterprise, you cannot use the VirusScan Enterprise installation utility to install these products at a later time. To do so, you must run the stand-alone Alert Manager or Desktop Firewall installer. See the *Alert Manager Product Guide* and the *Desktop Firewall Product Guide* for more information.

6 Click **Next** to continue.

7 In the **Product Configuration** dialog box, choose whether to import a repository list and whether to enable the on-access scanner when the installation completes:

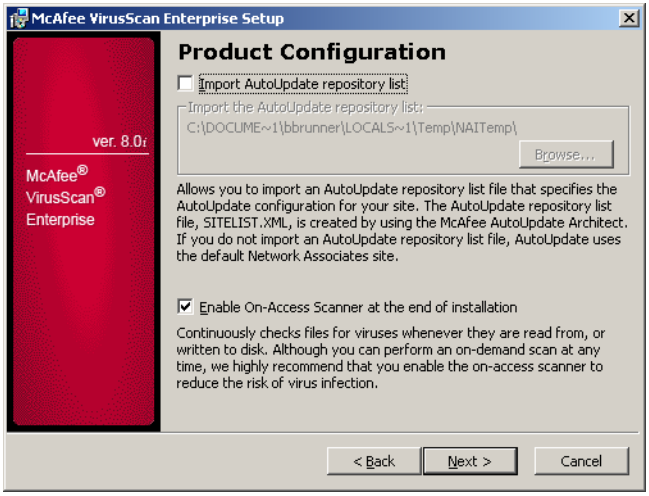
McAfee VirusScan Enterprise Setup
Product Configuration
Import AutoUpdate repository list
Import the AutoUpdate repository list:
C:\DOCUME~1\bbrunner\LOCALS~1\Temp\NAITemp\
Browse...
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Allows you to import an AutoUpdate repository list file that specifies the AutoUpdate configuration for your site. The AutoUpdate repository list file, SITELIST.XML, is created by using the McAfee AutoUpdate Architect. If you do not import an AutoUpdate repository list file, AutoUpdate uses the default Network Associates site.
Enable On-Access Scanner at the end of installation
Continuously checks files for viruses whenever they are read from, or written to disk. Although you can perform an on-demand scan at any time, we highly recommend that you enable the on-access scanner to reduce the risk of virus infection.
< Back
Next >
Cancel

Figure 2-11. Product Configuration

- **Import AutoUpdate repository list**. Select this option to import the repository list from the location you specify. The repository list must be located on a local drive; it cannot be imported from a mapped or a network drive.

  NOTE
  This option is selected by default only if a repository list is included in the installation file (.MSI) or the command-line property (cmasourcedir) has been set to a new location to point to the SITELIST.XML file.

  Accept the default location or click **Browse** to select a new location.

  NOTE
  If you do not import a repository list at this time, and one resides in the installation folder, it will be imported even though you do not select this option. If a repository list is not imported, AutoUpdate performs updates using the default McAfee Security site as its repository list.

  See the *Updating* section in the *VirusScan Enterprise Product Guide* for more information about the repository list.

- **Enable On-Access Scanner at the end of installation** *(Default)*. When selected, the on-access scanner automatically starts upon completion of the installation process.

8 Click **Next** to continue.

9 In the **Security Configuration** dialog box, you can set a password and specify which menu items users can see.

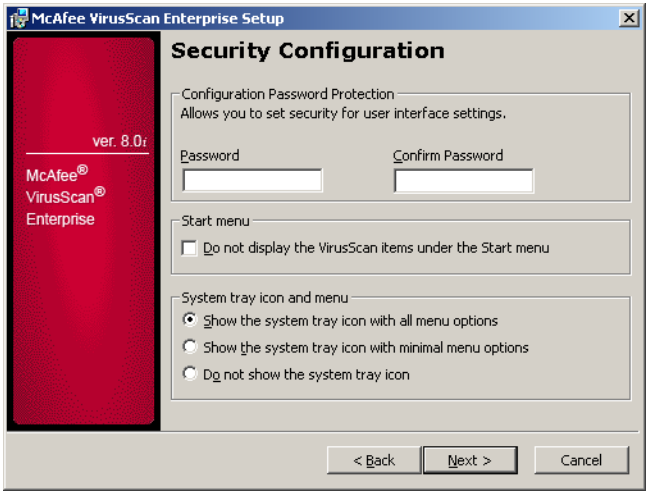
McAfee VirusScan Enterprise Setup
Security Configuration
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Configuration Password Protection
Allows you to set security for user interface settings.
Password
Confirm Password
Start menu
Do not display the VirusScan items under the Start menu
System tray icon and menu
Show the system tray icon with all menu options
Show the system tray icon with minimal menu options
Do not show the system tray icon
< Back
Next >
Cancel

Figure 2-12. Security Configuration

a Under **Configuration Password Protection**, type and confirm the user interface password to require a password for user interface settings. Leave these blank if you do not require a password.

b Under **Start menu**, select **Do not display the VirusScan items under the Start menu** if desired.

c Under **System tray icon and menu**, choose one of these options:

- **Show the system tray icon with all menu options** *(Default).* Display all menu items on the system tray icon menu.
- **Show the system tray icon with minimal menu options.** Limit the menu items users can see on the system tray icon menu to **About VirusScan Enterprise** and **On-Access Scan Statistics**.
- **Do not show the system tray icon**. Prevent users from accessing the system tray icon menu.

NOTE
After installation, you can set or reset password protection and system tray icon options from the **VirusScan Console**. See *Setting user interface options* in the *VirusScan Enterprise Product Guide* for more information.

10 Click **Next** to continue.

11 In the **Ready to install** dialog box, click **Install** if you are satisfied with all of the installation settings you selected.

NOTE
To review or change any of the settings, click **Back**, then return to the **Ready to install** dialog box and click **Install.**

The **Installing McAfee VirusScan Enterprise** dialog box shows the status of the installation.

12 In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to run an update task and/or an on-demand scan task upon completion of installation.

McAfee VirusScan Enterprise Setup
ver. 8.0i
McAfee®
VirusScan®
Enterprise
McAfee VirusScan Enterprise setup has completed successfully.
Allows you to update your virus definition (DAT) files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.
Update Now
Automatically checks for updates of virus defintion (DAT) files and/or scan engine and downloads any available updates.
Run On-Demand Scan
Examines all fixed drives for infected files. Infections are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\.
Finish
Cancel

Figure 2-13. Setup completed successfully — update and scan options

- **Update Now** *(Default).* When selected, an update task is automatically performed upon completion of installation.
- **Run On-Demand Scan** *(Default).* When selected, an on-demand scan task is automatically performed upon completion of installation.

13 Click **Finish**.

NOTE
Depending on the options you selected in Step 4, the program may run the update program or an on-demand scan at this time. If you selected both options, the update task runs first, then the on-demand scan task runs.

14 You are prompted to restart your computer to load the network driver.

McAfee VirusScan Enterprise Setup
The network driver is installed but you must restart the computer in order to load it.
Port Blocking, Infection Trace, and Infection Trace Blocking are disabled until the computer is restarted.
OK

Figure 2-14. Load network driver

WARNING
You must restart the computer to load the network driver. Loading this network driver enables the Port Blocking, Infection Trace, and Infection Trace Blocking features in VirusScan Enterprise.

Click **OK**, then restart the computer.

15 You may be prompted to restart your computer again when the installation process completes. If so, the **VirusScan Enterprise Setup** dialog box appears. You can choose to restart at this time or at a later time.

Using the command line to install program files

The VirusScan Enterprise Setup utility runs as a Microsoft Installer (.MSI) application, providing many custom installation options. Running the Setup utility from the command line allows you to customize the installation so that it runs the way you want and installs exactly the product features you want.

Review the *System requirements* on page 8 before you begin the installation process.

> **NOTE**
> You can run Setup from the command line to install the VirusScan Enterprise software to your *local* computer, but only if you have local administrator rights.

These topics are included in this section:

- *Command-line syntax* on page 34.
- *Installation scenarios* on page 34.
- *Logging installation progress* on page 36.
- *Installation properties* on page 37.
- *Selecting features* on page 40.
- *Setting restart options* on page 41.

Command-line syntax

To install the product from the command line:

1. Open the Windows command-line component with one of these methods:
   - Select **Command Prompt** from the **Start** menu.
   - Select **Run** from the **Start** menu.
2. Type the command line either at the command prompt or in the **Run** dialog box.

   The Setup command-line syntax looks like this:

   ```
   setup PROPERTY=VALUE[,VALUE] [/option]
   ```

   This syntax does not require any specific order in its elements, except that you may not separate a property and its value. The syntax consists of:

   - **File name** — The name of the executable file, `SETUP.EXE`.
   - **Options** — Each option is preceded by a forward slash (/) character and is *not* case-sensitive. The installation scenarios that appear later in this guide discuss some of the available options.
   - **Properties** — Use properties to determine how the installation runs. Each property consists of:
     - A name, which must appear in uppercase letters.
     - An equal (=) sign.
     - One or more values, each separated by commas. Most property values must appear in uppercase letters, but some, such as True and False, must appear in mixed case. The Microsoft Installer permits a variety of properties that determine how your installation runs. To learn about those properties, see the Microsoft Installer documentation.

Installation scenarios

Use these scenarios to customize your installation:

- Installing silently.
- Installing to a custom location.

Installing silently

Use command-line options to set up VirusScan Enterprise software on each network node with little or no interaction from users. During a silent installation, Setup does not display the installation wizard, or offer the user any configuration options. Instead, you pre-configure those choices and run Setup in the background on each destination computer. You can install VirusScan Enterprise software on any unattended computer with or without the user's knowledge, provided you have the necessary administrator rights.

For example, use the `/q` option to specify the user interface.

Add these options to run a silent or semi-silent installation:

Option	Function
`q or qn`	Silent installation. Nothing displays during installation.
`qb`	Basic user interface. Use qb! to hide the Cancel button.
`qb+`	Basic user interface with a modal dialog box displayed at the end of installation. Use qb+! or qb!+ to hide the Cancel button.The modal dialog box is not displayed if the user cancels the installation.
`qb-`	Basic user interface with no modal dialog boxes. Use qb-! or qb!- to hide the Cancel button.
`qf`	Full user interface and any authored FatalError, UserExit, or Exit modal dialog displayed at the end of installation.
`qn+`	No user interface except for a modal dialog box displayed at the end of installation.
`qr`	Reduced user interface with no modal dialog displayed at the end of installation.

Installing to a custom location

To install VirusScan Enterprise software to a custom location, add the INSTALLDIR property to specify the location you want to use. For example, to silently install VirusScan Enterprise software to C:\My Anti-Virus Software, type this line at the command prompt:

```
setup INSTALLDIR="c:\My Anti-Virus Software" /q
```

Use quotes only if the destination name has spaces.

Logging installation progress

To record installation progress in a log file, add this option and parameter to the Setup command line:

```
/l*v "c:\temp\log.txt"
```

Here, `c:\temp\log.txt` can be any location and any file name you want to use to create the log file. This option logs all installer activity, including all files copied, all registry keys added, and all .INI file changes.

Replace the asterisk (*) shown in the command-line example, with one or more of these parameters to limit the type of data that the log file records:

Option	Description
i	status messages
w	non-fatal warnings
e	all error messages
a	action starts
r	action-specific records
u	user requests
c	initial user interface parameters
m	out-of-memory or fatal exit information
o	out-of-disk-space messages
p	terminal properties
+	append to existing file
!	flush each line to the log

Installation properties

Use these properties to customize the command-line installation:

Property	Function
ADDLOCAL	Installs specific features to the local computer.
AMGSOURCEDIR	Sets the default Alert Manager source path. In the SETUP.INI, the default path is \AMG. Specify the path in the SETUP.INI. For example on the command line, a fixed path is: AMGSOURCEDIR=C:\AMG **Note:** The path is relative to where VirusScan Enterprise is installed from.
CMASOURCEDIR	Set the source path for the SITELIST.XML. The default path is: %TEMP%\NAITemp. **Note:** The repository list must be located on a local drive and cannot be imported from a mapped or a network drive.
DFWSOURCEDIR	Sets the default Desktop Firewall source path. In the SETUP.INI, the default path is \DFW. Specify the path in the SETUP.INI. For example on the command line, a fixed path is: DFWSOURCEDIR=C:\DFW **Note:** The path is relative to where VirusScan Enterprise is installed from.
ENABLEONACCESSSCANNER	False = A False value cannot be set. True = Enable on-access scanner upon completion of installation (Default). **Note:** If you do not want to enable the on-access scanner, set the property to "", an empty string. For example: ENABLEONACCESSSCANNER=""
EXTRADATSOURCEDIR	Set the source path for the EXTRA.DAT. During installation, the EXTRA.DAT is copied into the location where the engine files reside.
FORCEAMSINSTALL	True = Install Alert Manager, if present.
INSTALLDIR	Specifies the installation folder. The value consists of the installation path.

Property	Function
LOCKDOWNVIURUSSCANSHORTCUTS	False = A False value cannot be set. True = Do not display any shortcuts under the **Start** menu. The default is an empty string. **Note:** To allow the shortcuts to be installed, set the property to "", an empty string. For example: LOCKDOWNVIRUSSCANSHORTCUTS=""
PRESERVESETTINGS	Preserves settings when upgrading from NetShield, VirusScan, or an earlier version of VirusScan Enterprise. False = A False value cannot be set. True = Preserve settings (Default). **Note:** If you do not want to preserve settings, set the property to "", an empty string. For example: PRESERVESETTINGS=""
REBOOT	Specifies whether Setup should restart your computer. You can force the computer to restart if it is required, or prevent it from restarting.
REMOVE	Removes one or more program features. You can specify a feature, or use the value ALL to remove all features. If you combine this property with the ADDLOCAL property, you can install all but one or two specific features
REMOVEINCOMPATIBLESOFTWARE	Removes competitor's anti-virus software that could conflict with this VirusScan Enterprise version. By default, its value is True.
RUNAUTOUPDATE	False = A False value cannot be set. True = Run update upon completion of installation (Default). **Note:** If you do not want to run update upon completion of installation, set the property to "", an empty string. For example: RUNAUTOUPDATE=""

Property	Function
RUNAUTOUPDATESILENTLY	False = A False value cannot be set. True = Run silent update upon completion of installation. The default is an empty string. **Note:** If you do not want to run a silent update upon completion of installation, set the property to "", an empty string. For example: RUNAUTOUPATESILENTLY=""
RUNONDEMANDSCAN	False = A False value cannot be set. True = Run a scan of all local drives upon completion of installation (Default). **Note:** If you do not want to run the on-demand scanner at completion of installation, set the property to "", an empty string. For example: RUNONDEMANDSCAN=""
RUNONDEMANDSCANSILENTLY	False = A False value cannot be set. True = Run on-demand scan silently upon completion of installation. The default is an empty string. **Note:** If you do not want to run a silent on-demand scan upon completion of installation, set the property to "", an empty string. For example: RUNONDEMANDSCANSILENTLY=""

Selecting features

When you run Setup from the command line to install specific program features, the utility installs those features according to a pre-existing hierarchy. This means that if you choose to install only the VirusScan Enterprise shell extensions, for example, Setup knows that you must have the on-demand scanner application installed to use the extensions. It therefore installs both this file and any related files.

To specify individual features, Setup requires that you add specific feature names as command-line parameters. The feature names you can specify from the command line are:

Feature	Description
`Console`	The VirusScan Console.
`AutoUpdate`	The AutoUpdate utility.
`LotusNotesScan`	The Lotus Notes e-mail scanner.
`EmailScan`	The Microsoft Outlook e-mail scanner.
`OnAccessScanner`	The on-access scanner.
`BufferOverflow`	The buffer overflow protection feature. Note: This feature cannot be installed on 64-bit systems or if either the Entercept agent or the Cisco Security agent are found on the local computer.
`ScriptScan`	The script scanner. Note: This feature cannot be installed on 64-bit systems.
`OnDemandScanner`	The on-demand scanner.
`ShellExtensions`	Extensions that add right-click functionality that enables you to scan individual files. Note: This feature cannot be installed on 64-bit systems.

- To use these feature names in a command line, specify the destination and the feature name. You can specify features or use the `ALL` property to install all of the features. For a complete installation, type this line at the command prompt:

  ```
  setup.exe ADDLOCAL=ALL /q
  ```

- Use a comma to separate values when installing more than one feature. To add the on-demand scanner and the on-access scanner together, type this line at the command prompt:

  ```
  setup.exe ADDLOCAL=OnAccessScanner,OnDemandScanner /q
  ```

- To remove all VirusScan Enterprise components, type this line at the command prompt:

  ```
  setup.exe REMOVE=ALL /q
  ```

- To install all features except one, for example the on-demand scanning feature, type this line at the command prompt:

```
setup.exe ADDLOCAL=ALL REMOVE=OnDemandScanner /q
```

- You can also choose different features for an installation that you do not run silently. If, for example, you omit the `/q` option in any of the command line examples shown, the Custom Setup wizard dialog box shows only the features you specify as those available for installation. If you use these same examples to specify a feature set for installation, Setup installs only the features you specified during a **Typical** installation.

Setting restart options

You can force a restart if one is required, or prevent the destination computer from restarting during the installation. To do this, add the REBOOT property to the command line:

- `REBOOT=F` forces the restart if one is required.
- `REBOOT=R` prevents the restart.

To run a silent installation and prevent a system restart:

```
setup REBOOT=R /q
```

Using a login script to install program files

To install VirusScan Enterprise software at the time each of your destination computers starts, add a Setup command line to your login script and include all of the options and properties for governing how Setup runs. For example, you can add a property to look for the VirusScan Enterprise default program location.

To use a login script for this purpose, you must also copy or "push" the VirusScan Enterprise installation package to a local location on the destination computer. You may *not* use a login script to install VirusScan Enterprise software from elsewhere on your network.

Incompatible software removed

By default, Setup removes incompatible software before it installs the VirusScan Enterprise software. These products are removed:

Alert Manager 4.6.0

CA eTrust AntiVirus

CA eTrust InoculateIT

Dr. Solomon's Anti-Virus 8.5.0

Dr. Solomon's NetShield 4.03

Dr. Solomon's NetShield 4.5.0

Dr. Solomon's VirusScan 4.0.1

Dr. Solomon's VirusScan 4.0.2

Dr. Solomon's VirusScan 4.0.3

McAfee Firewall 3.0

McAfee Firewall 4.0

McAfee NetShield 4.02

McAfee NetShield 4.03

McAfee VirusScan ASAP

McAfee VirusScan Home Edition 7.0

McAfee VirusScan Online

McAfee VirusScan TC

McAfee VirusScan 4.0.1

McAfee VirusScan 4.0.2

McAfee VirusScan 4.0.2 (Windows NT products)

McAfee VirusScan 4.0.3 (Windows 9x products)

McAfee VirusScan 4.0.3 (Windows NT products)

McAfee VirusScan 4.5.0

McAfee VirusScan 4.5.1 (English, Japenese)

McAfee VirusScan 4.5.1 (German, French, Spanish, Italian, Dutch, Portuguese, Swedish, Polish, Traditional Chinese, Simplified Chinese, Korean)

McAfee VirusScan 5.1.x

McAfee VirusScan 5.2.x

McAfee VirusScan 6.0

Norton AntiVirus 2002

Norton AntiVirus 2003 (Full install)

Norton AntiVirus 2003 (Preinstall version)

Norton AntiVirus 8.x for Windows NT (client)

Norton AntiVirus 8.x for Windows NT (server)

Norton AntiVirus 9.x for Windows NT

Norton AntiVirus Corporate Edition 7.0 for Windows NT

Norton AntiVirus Corporate Edition 7.x for NT Server

Norton AntiVirus Corporate Edition 7.x for Windows 9x/NT

Norton AntiVirus Corporate Edition for Windows 7.0

Norton Internet Security (Symantec Corporation)

Norton Mobile Update Distribution Console

Norton Rescue Disk

Panda AdminSecure

Panda Antivirus 6.0 Platinum

Panda Antivirus Titanium

Panda Platinum Internet Security

Panda Titanium AntiVirus 2004

Pc-cillin 2000 for NT

Pc-cillin 2002/VirusBuster

Sophos Anti-Virus version 3.x

Trend Micro Internet Security

Trend Micro OfficeScan Corporate Edition 5.x

Trend Office Scan

Trend Office Scan 3.51

Trend Office Scan95 3.51

Trend PC-cillin 2000

Trend PC-cillin/VirusBuster 2003

Trend ServerProtect 4.8

Trend ServerProtect 5.x

V3Net for Windows Server

V3Pro 2002 Deluxe

Files installed

During installation, files are installed in various locations. One of the locations is the installation path which is determined during installation. The default installation path is:

```
<drive>:\Program Files\Network Associates\
```

Files are installed in these folders:

- *VirusScan folder* on page 44.
- *Resources folder* on page 45.
- *Engine folder* on page 45.

VirusScan folder

These files are installed to the VirusScan folder in the installation path:

AdsLokUU.Dll	license.bin	naiavfin.exe	shcfg32.exe
avf.exe	logparser.exe	naicondl.dll	shext.dll
BBCpl.dll	mcconsol.exe	naiconsl.dll	shstat.exe
bho.dll	Mcshield.exe	NaiEvent.dll	shutil.dll
bo.rul	mcupdate.exe	nailite.dll	vscan.bof
coptcpl.dll	Mcvssnmp.dll	naiwmain.dll	VSIDSvr.dll
csscan.exe	MERTool.url	nvpcpl.dll	vsodscpl.dll
dssdata.h	midutil.dll	OASCpl.dll	VSPlugin.dll
DSSDATA.INI	mvstdi5x.sys	Packing.lst	VSTskMgr.exe
EmCfgCpl.dll	mytilus.dll	readme.txt	vsupdate.dll
EntSrv.dll	NaEventU.Dll	scan32.exe	vsupdcpl.dll
entvutil.exe	naiann.dll	ScanEmal.dll	
ftcfg.dll	naiavf5x.cat	ScnCfg32.exe	
ftl.dll	naiavf5x.inf	scriptproxy.dll	
graphics.dll	naiavf5x.sys	Additional Preserved Settings	

If you are using Lotus Notes, these files are also installed to the VirusScan folder in the installation path:

ncdaemon.exe	ncinstall.dll	ncres.dll	nctrace.dll
ncextmgr.dll	ncmenu.dll	ncscan.dll	

Resources folder

The resources folder is named differently depending on the language being installed. For example, the English resources folder is named Res09. These files are installed to the resources folder in the installation path:

alertres.dll	Product.DLL	ShStat.DLL	vse.chm
McShield.DLL	SEmalRes.Dll	ShUtilRc.DLL	VsTskMgr.DLL
mcupdate.DLL	ShCfg32.DLL	strings.bin	
NaEvtRes.Dll	shextres.dll	AMG.chm (if Alert Manager installed)	

Engine folder

These files are installed to the Engine folder which is located at:

```
<drive>:\Program Files\Common Files\Network Associates\
```

Avparam.dll	Mcscan32.dll	scan.dat
Clean.dat	Messages.dat	scan.exe
license.dat	Names.dat	SignLic.Txt

Testing your installation

Once installed, the software can scan your system for infected files. You can test whether it is installed correctly and can properly scan for viruses by implementing a test developed by the European Institute for Computer Anti-Virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation:

1. Using a standard Windows text editor such as Notepad, type the following string, *on a single line with no spaces or line breaks*:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

2. Save the file with the name EICAR.COM. The file size is 68 bytes. Make a note of the folder in which you saved the file.

3. Start the program.

4. To test the on-demand scanner, create an on-demand scan task that examines the folder where you saved EICAR.COM. When the scanner examines this file, it reports finding the EICAR test file.

5. To test the on-access scanner, confirm that the on-access scanner is configured to scan files written to the computer and files read from the computer. See *Configuring the on-access scanner* in the *VirusScan Enterprise Product Guide* for additional information. Locate the EICAR.COM file and try to copy or move it to another location. The scanner reports finding the EICAR test file when it examines the file.

   NOTE
   This file is *not a virus*—it cannot spread, infect other files, or harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Modifying or Repairing the Software 3

You can modify, repair, or reinstall the VirusScan Enterprise program files using the program maintenance feature.

These topics are included in this section:

- *Modifying installed features* on page 48.
- *Reinstalling or repairing program files* on page 53.

Modifying installed features

Change which program features are installed.

These topics are included in this section:

- *Using the Setup utility to modify features* on page 48.
- *Using the command line to modify program features* on page 52.

Using the Setup utility to modify features

1 Start the Setup utility with one of these methods.

- From the product CD:
  - a Insert the CD into the CD-ROM drive.
  - b Click **Install** from the **Welcome** dialog box.
- From the command line:
  - a Click **Start**, then select **Run**.
  - b Type `<X>:\SETUP.EXE` in the **Run** dialog box, then click **OK**.

    Here, `<X>:` represents the drive letter for your CD-ROM, or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click **Browse**. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.
- From the installation folder:
  - a Browse to the location where you installed the program files.
  - b Double-click SETUP.EXE.

2 In the **Program Maintenance** dialog box, select **Modify**.

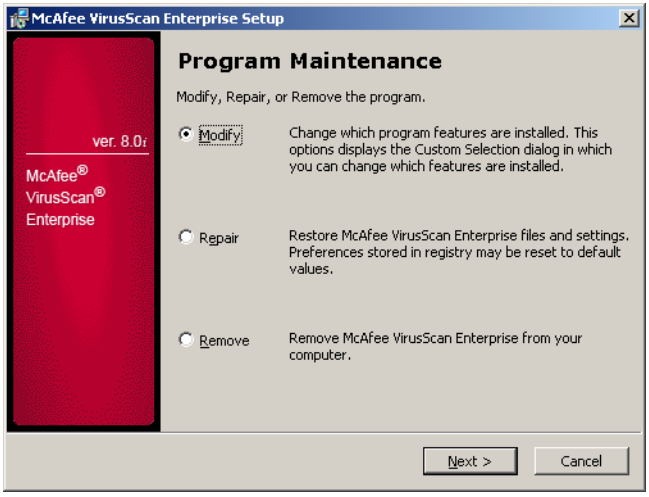
McAfee VirusScan Enterprise Setup
Program Maintenance
Modify, Repair, or Remove the program.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Modify
Change which program features are installed. This options displays the Custom Selection dialog in which you can change which features are installed.
Repair
Restore McAfee VirusScan Enterprise files and settings. Preferences stored in registry may be reset to default values.
Remove
Remove McAfee VirusScan Enterprise from your computer.
Next >
Cancel

Figure 3-1. Modify program features

3 Click **Next**.

4 In the **Feature Selection** dialog box select which features you want to modify.

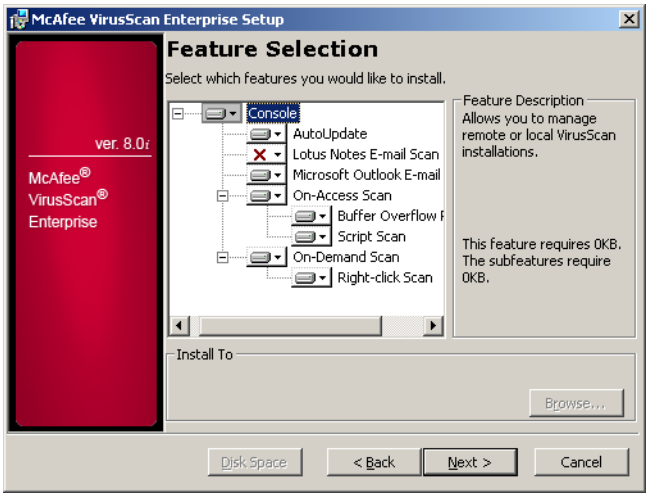

Figure 3-2. Feature Selection — Modify

a Under **Select which features you would like to install**, these features are available for selection:

- **Console** (Default)
- **AutoUpdate**
- **Lotus Notes E-mail Scan**
- **Microsoft Outlook E-mail Scan**
- **On-Access Scan**

  Buffer Overflow Protection

  NOTE
  This feature cannot be installed on 64-bit systems or if either the Entercept agent or the Cisco Security agent are found on the local computer.

  Script Scan

  NOTE
  This feature cannot be installed on 64-bit systems.

- **On-Demand Scan**

  Right-click Scan

  NOTE
  This feature cannot be installed on 64-bit systems.

b For each selected feature, you can also select a corresponding action from the drop-down menu. Click next to the selected feature, to display the action menu, then select the action for that feature.

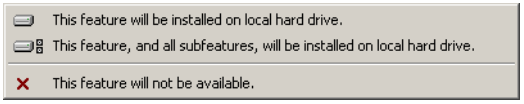
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Figure 3-3. Feature action options

c Under **Install To**, accept the default path, type a new path, or click **Browse** to select a path.

5 Click **Next** to continue.

> **NOTE**
> The **Install To** path and **Disk Space** features are disabled. To change the installation path, you must first remove the product, then reinstall the product to the required path.

6 Click **Next** to open the **Ready to install** dialog box.

7 In the **Ready to install** dialog box, click **Install** if you are satisfied with all of the installation settings you selected.

> **NOTE**
> To review or change any of the settings, click **Back**, then return to the **Ready to install** dialog box and click **Install.**

8 When the installation process completes successfully, click **Finish**.

Using the command line to modify program features

1 Open the Windows command-line component with one of these methods:

- Select **Command Prompt** from the **Start** menu.
- Select **Run** from the **Start** menu.

2 Type the command line at the command prompt or in the **Run** dialog box.

Command-line syntax

To add a feature, use ADDLOCAL=FEATURENAME.

The command-line syntax for a adding a feature looks like this:

```
setup.exe ADDLOCAL=OnAccessScanner,OnDemandScanner/q
```

To delete a feature, use REMOVE=FEATURENAME.

The command-line syntax for removing a feature looks like this:

```
setup.exe REMOVE=OnAccessScanner,OnDemandScanner/q
```

Features

These features can be installed or removed individually using a comma-separated list, or you can specify the ALL property:

Feature	Description
Console	The VirusScan Console.
AutoUpdate	The AutoUpdate utility.
LotusNotesScan	The Lotus Notes e-mail scanner.
EmailScan	The Microsoft Outlook e-mail scanner.
OnAccessScanner	The on-access scanner.
BufferOverflow	The buffer overflow protection feature. Note: This feature cannot be installed on 64-bit systems or if either the Entercept agent or the Cisco Security agent are found on the local computer.
ScriptScan	The script scanner. Note: This feature cannot be installed on 64-bit systems.
OnDemandScanner	The on-demand scanner.
ShellExtensions	Extensions that add right-click functionality that enables you to scan individual files. Note: This feature cannot be installed on 64-bit systems.

Reinstalling or repairing program files

Reinstall or repair product features.

These topics are included in this section:

- *Using the Setup utility to reinstall or repair program files* on page 53.
- *Using the command line to reinstall or repair the program files* on page 59.

Using the Setup utility to reinstall or repair program files

1. Start the Setup utility with one of these methods.
   - From the product CD:
     a. Insert the CD into the CD-ROM drive.
     b. Click **Install** from the **Welcome** dialog box.
   - From the command line:
     a. Click **Start**, then select **Run**.
     b. Type `<X>:\SETUP.EXE` in the **Run** dialog box, then click **OK**.

        Here, `<X>:` represents the drive letter for your CD-ROM, or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click **Browse**. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.
   - From the installation folder:
     a. Browse to the location where you installed the program files.
     b. Double-click SETUP.EXE.

2 In the **Program Maintenance** dialog box, select **Repair**.

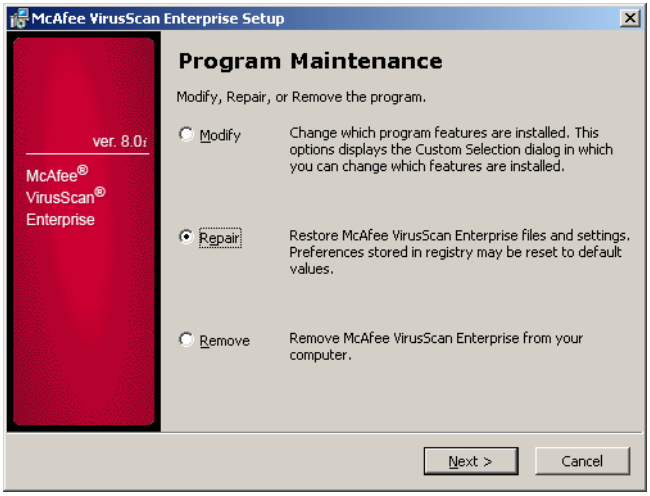
McAfee VirusScan Enterprise Setup
Program Maintenance
Modify, Repair, or Remove the program.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Modify
Change which program features are installed. This options displays the Custom Selection dialog in which you can change which features are installed.
Repair
Restore McAfee VirusScan Enterprise files and settings. Preferences stored in registry may be reset to default values.
Remove
Remove McAfee VirusScan Enterprise from your computer.
Next >
Cancel

Figure 3-4. Repair program files

3 Click **Next**.

4 In the **Reinstall or Repair the Product** dialog box, choose from these options:

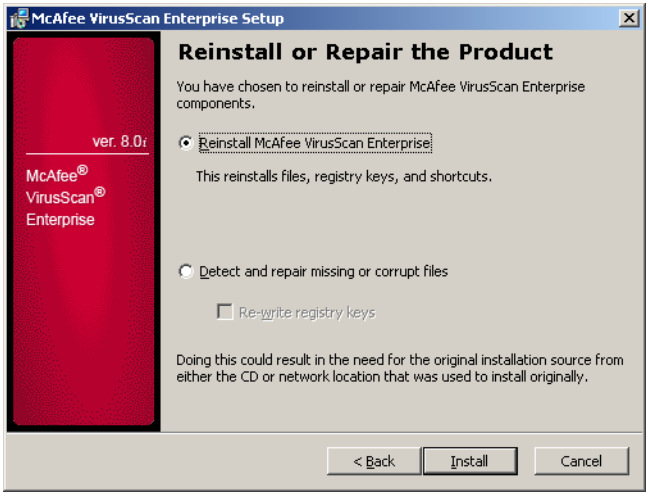
McAfee VirusScan Enterprise Setup
Reinstall or Repair the Product
You have chosen to reinstall or repair McAfee VirusScan Enterprise components.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Reinstall McAfee VirusScan Enterprise
This reinstalls files, registry keys, and shortcuts.
Detect and repair missing or corrupt files
Re-write registry keys
Doing this could result in the need for the original installation source from either the CD or network location that was used to install originally.
< Back
Install
Cancel

Figure 3-5. Reinstall or Repair the Product

- **Reinstall McAfee VirusScan Enterprise**. Reinstalls the VirusScan Enterprise program files, registry keys, and shortcuts. See *Reinstalling program files* on page 55 to continue this procedure.
- **Detect and repair missing or corrupt files**. Repairs the VirusScan Enterprise program files. See *Repairing program files* on page 57 to continue this procedure.

Reinstalling program files

1 From the **Reinstall or Repair the Product** dialog box, select **Reinstall McAfee VirusScan Enterprise.**

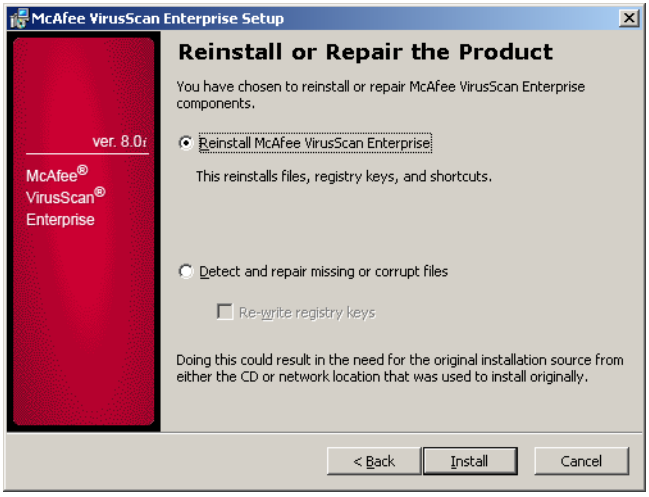
McAfee VirusScan Enterprise Setup
Reinstall or Repair the Product
You have chosen to reinstall or repair McAfee VirusScan Enterprise components.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Reinstall McAfee VirusScan Enterprise
This reinstalls files, registry keys, and shortcuts.
Detect and repair missing or corrupt files
Re-write registry keys
Doing this could result in the need for the original installation source from either the CD or network location that was used to install originally.
< Back
Install
Cancel

Figure 3-6. Reinstall program files

2 Click **Install**.

The **Installing McAfee VirusScan Enterprise** dialog box appears and shows the status of the installation.

3 In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to run an update task and/or an on-demand scan task upon completion of installation.

McAfee VirusScan Enterprise Setup
ver. 8.0i
McAfee®
VirusScan®
Enterprise
McAfee VirusScan Enterprise setup has completed successfully.
Allows you to update your virus definition (DAT) files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.
Update Now
Automatically checks for updates of virus defintion (DAT) files and/or scan engine and downloads any available updates.
Run On-Demand Scan
Examines all fixed drives for infected files. Infections are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\.
Finish
Cancel

Figure 3-7. Setup completed successfully — update and scan options

- **Update Now** *(Default).* When selected, an update task is automatically performed upon completion of installation.
- **Run On-Demand Scan** *(Default).* When selected, an on-demand scan task is automatically performed upon completion of installation.

4 Click **Finish**.

> **NOTE**
> Depending on the options you selected in Step 3, the program may run the update program or an on-demand scan at this time. If you select both options, the update task runs first, then the on-demand scan task runs.

5 You may be prompted to restart your computer. If so, the **VirusScan Enterprise Setup** dialog box appears. You can choose to restart at this time, or restart after the installation completes.

Repairing program files

WARNING

If you manually remove or rename any of the program files, the repair feature may fail. See the *Troubleshooting* appendix in the *VirusScan Enterprise Product Guide* for detailed instructions about trying to repair files after they have been removed or renamed.

1 From the **Reinstall or Repair the Product** dialog box, select **Detect and repair missing or corrupt files.**

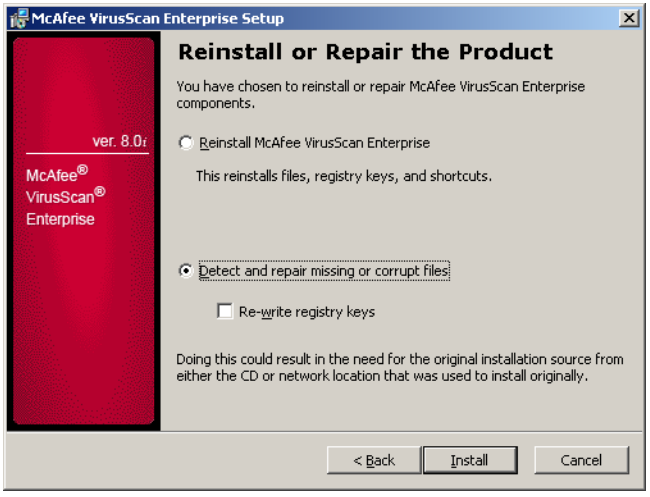
McAfee VirusScan Enterprise Setup
Reinstall or Repair the Product
You have chosen to reinstall or repair McAfee VirusScan Enterprise components.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Reinstall McAfee VirusScan Enterprise
This reinstalls files, registry keys, and shortcuts.
Detect and repair missing or corrupt files
Re-write registry keys
Doing this could result in the need for the original installation source from either the CD or network location that was used to install originally.
< Back
Install
Cancel

Figure 3-8. Detect and repair files

2 Select **Re-write registry keys** to perform this function during the repair process.

WARNING

Neither the **Reinstall McAfee VirusScan Enterprise** nor the **Detect and repair missing or corrupt files** features supports reinstalling or repairing update components. If an AutoUpdate file is removed or corrupted, you must remove the AutoUpdate component, then reinstall it.

For information about using the Setup utility or the command line to remove components, see *Removing the Software* on page 61.

3 Click **Install**.

The **Installing McAfee VirusScan Enterprise** dialog box shows the status of the installation.

4 In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to run an update task and/or an on-demand scan task upon completion of installation.

McAfee VirusScan Enterprise Setup
McAfee VirusScan Enterprise setup has completed successfully.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Allows you to update your virus definition (DAT) files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.
Update Now
Automatically checks for updates of virus defintion (DAT) files and/or scan engine and downloads any available updates.
Run On-Demand Scan
Examines all fixed drives for infected files. Infections are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\.
Finish
Cancel

Figure 3-9. Setup completed successfully — update and scan options

- **Update Now** *(Default).* When selected, an update task is automatically performed upon completion of installation.
- **Run On-Demand Scan** *(Default).* When selected, an on-demand scan task is automatically performed upon completion of installation

5 Click **Finish**.

> **NOTE**
> Depending on the options you selected in Step 4, the program may run the update program or an on-demand scan at this time. If you select both options, the update task runs first, then the on-demand scan task runs.

6 You may be prompted to restart your computer. If so, the **VirusScan Enterprise Setup** dialog box appears. You can choose to restart at this time, or restart after the installation completes.

Using the command line to reinstall or repair the program files

1 Open the Windows command-line component with one of these methods:

- Select **Command Prompt** from the **Start** menu.
- Select **Run** from the **Start** menu.

2 Type the command line at the command prompt or in the **Run** dialog box.

Command-line syntax

The command-line syntax for a reinstallation looks like this:

```
msiexec /I{product code}REINSTALL=[feature]REINSTALLMODE=[option]
```

The command-line syntax for a repair looks like this:

```
msiexec /f[option]{product code}
```

Features

These features can be installed individually using a comma-separated list, or you can specify the ALL property:

Feature	Description
Console	The VirusScan Console.
AutoUpdate	The AutoUpdate utility.
LotusNotesScan	The Lotus Notes e-mail scanner.
EmailScan	The Microsoft Outlook e-mail scanner.
OnAccessScanner	The on-access scanner.
BufferOverflow	The buffer overflow protection feature. Note: This feature cannot be installed on 64-bit systems or if either the Entercept agent or the Cisco Security agent are found on the local computer.
ScriptScan	The script scanner. Note: This feature cannot be installed on 64-bit systems.
OnDemandScanner	The on-demand scanner.
ShellExtensions	Extensions that add right-click functionality that enables you to scan individual files. Note: This feature cannot be installed on 64-bit systems.

Command-line options

You can use any combination of these options:

Option	Description
p	Reinstall only if file is missing.
o	Reinstall if file is missing or if an older version is installed.
e	Reinstall if file is missing or an equal or older version is installed.
d	Reinstall if file is missing or a different version is installed.
c	Reinstall if file is missing, or if the stored checksum does not match the calculated value. Only repairs files that have msidbFileAttributesChecksum in the Attributes column of the File table.
a	Force all files to be reinstalled.
u	Rewrite all required user-specified registry entries.
m	Rewrite all required system-specific registry entries.
s	Overwrite all existing shortcuts.
p	Run from source and re-cache the local package.
	Reinstall only if file is missing.

Removing the Software 4

Remove the VirusScan Enterprise program files with one of these methods:

- *Using the Setup utility to remove the product* on page 62.
- *Using the command line to remove the product* on page 65.
- *Using the Add/Remove Programs utility to remove the product* on page 66.

Using the Setup utility to remove the product

1. Start the Setup utility using one of these methods.

   - From the product CD:

     a. Insert the CD into the CD-ROM drive.

     b. Click **Install** from the **Welcome** dialog box.

   - From the command line:

     a. Click **Start**, then select **Run**.

     b. Type `<X>:\SETUP.EXE` in the **Run** dialog box, then click **OK**.

     Here, `<X>:` represents the drive letter for your CD-ROM, or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click **Browse**. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.

   - From the installation folder:

     a. Browse to the location where you installed the program files.

     b. Double-click SETUP.EXE.

2 In the **Program Maintenance** dialog box, click **Remove**.

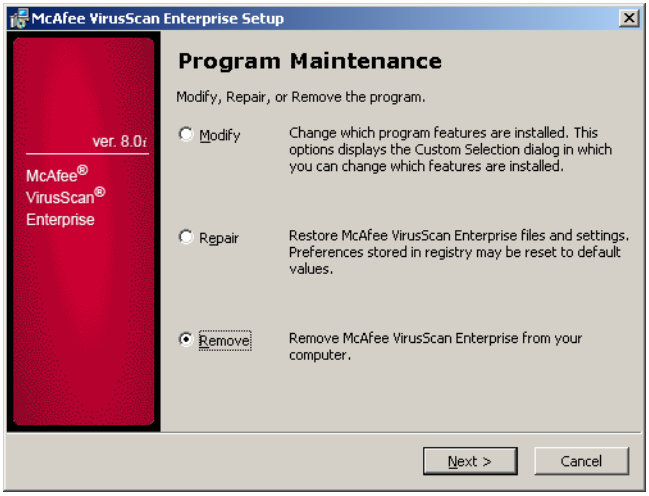
McAfee VirusScan Enterprise Setup
Program Maintenance
Modify, Repair, or Remove the program.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Modify
Change which program features are installed. This options displays the Custom Selection dialog in which you can change which features are installed.
Repair
Restore McAfee VirusScan Enterprise files and settings. Preferences stored in registry may be reset to default values.
Remove
Remove McAfee VirusScan Enterprise from your computer.
Next >
Cancel

Figure 4-1. Program Maintenance

3 Click **Next**.

4 In the **Remove McAfee VirusScan Enterprise** dialog, click **Remove**.

McAfee VirusScan Enterprise Setup
Remove McAfee VirusScan Enterprise
You have chosen to remove the program from your system.
ver. 8.0i
McAfee®
VirusScan®
Enterprise
Click Remove to remove McAfee VirusScan Enterprise from your computer. After removal, this program will no longer be available for use.
< Back
Remove
Cancel

Figure 4-2. Remove VirusScan Enterprise

5 When the removal process completes successfully, click **Finish**.

6 After VirusScan Enterprise is removed, there may be some remaining files or folders that are not removed.

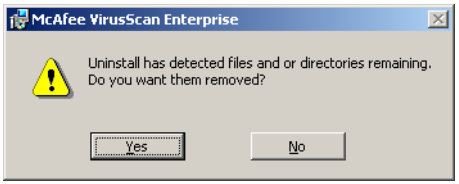

Figure 4-3. Remove remaining files and folders

These are files and folders which were not installed initially with the VirusScan Enterprise product, for example, log files or other files or folders that the user added. Two files that are used for debugging are left in the `%TEMP%\NAI LOGS` folder:

- VSEUninst.log
- VSEInst.log

Click **Yes** to remove the remaining files.

7 Restart your computer after the removal process completes.

WARNING
We strongly recommend that you restart your computer after removing files and before you reinstall the software.

When you remove files using Setup on the command line, some files or stopped services may not be removed. For example, if you remove the VirusScan Enterprise product while the Network Associates Task Manager or the Network Associates McShield services are stopped, these services are not removed. Restarting after removing files ensures that all files and services are removed before reinstalling the software.

Using the command line to remove the product

1. Open the Windows command-line component with one of these methods:
   - Select **Command Prompt** from the **Start** menu.
   - Select **Run** from the **Start** menu.
2. Type this string at the command prompt or in the **Run** dialog box.

   ```
   <X>:\SETUP.EXE /x
   ```

   Here, `<X>:` represents the drive letter for your CD-ROM or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click **Browse**. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.
3. Restart your computer after the removal process completes.

   WARNING
   We strongly recommend that you restart your computer after removing files and before you reinstall the software.

   When you remove files using Setup on the command line, some files or stopped services may not be removed. For example, if you remove the VirusScan Enterprise product while the Network Associates Task Manager or the Network Associates McShield services are stopped, these services are not removed. Restarting after removing files ensures that all files and services are removed before reinstalling the software.

Using the Add/Remove Programs utility to remove the product

Open the **Add/Remove Programs** utility that is included in the Windows Control Panel.

1. Click **Start**, then select **Settings** | **Control Panel** | **Add/Remove Programs**.
2. Select the VirusScan Enterprise program from the list of installed programs, then click **Remove**.
3. Restart your computer after the removal process completes.

WARNING

We strongly recommend that you restart your computer after removing files and before you reinstall the software.

When you remove files using Setup on the command line, some files or stopped services may not be removed. For example, if you remove the VirusScan Enterprise product while the Network Associates Task Manager or the Network Associates McShield services are stopped, these services are not removed. Restarting after removing files ensures that all files and services are removed before reinstalling the software.

Configuring Netopsystems' FEAD Optimizer A

The Netopsystems' FEAD Optimizer technology has been used to compress the VirusScan Enterprise installation file. This section provides details about recomposing the installation files from the command line.

These topics are included in this section:

- *Optimized file defaults*.
- *Command-line properties and switches* on page 68.

Optimized file defaults

These default actions are set:

Action	Default
Execution	Yes
Delete	Yes
Silent	No
Output folder	%TEMP%\McAfee VirusScan Enterprise

Command-line properties and switches

When executing Setup from the command line, command-line properties and switches can be used with an optimized file to customize the recomposing process of the destination file.

The syntax is:

```
setup.exe [<switches>...]
```

The switches are defined as:

```
<switches> = <Netopsystems' switches>|<VirusScan Enterprise
switches>
```

The VirusScan Enterprise switches are the parameters that you pass to the VirusScan Enterprise Setup utility. For example:

```
setup.exe -s -nos_d installdir="c:\abc def"/L

setup.exe nocdi=true -nos_o"d:\temp" -nos_s reboot=a
```

These command-line properties or switches may be used with an optimized file:

Property or switch	Function
`-nos_ne`	No execution — Extracts the files from the Setup utility but does not execute the Setup utility or delete the setup files.
`-nos_nd`	No delete — Does not remove the setup files after executing the Setup utility. If the `-nos_-ne` switch is also present, the `-nos_-nd` switch is overridden.
`-nos_d`	Delete — Removes the setup files after executing the Setup utility. If the `-nos_-ne` switch is also present, the `-nos_-d` switch is overridden.
`-nos_s`	Silent mode — Installs the setup files in silent mode. Installs automatically when using: `/s, /S, -s, -S, /q, /Q, -q, -Q.`
`-nos_o"<path>"`	Output folder — The folder to which you want to extract the setup files.

Index

A

audience for this manual, 13
AVERT (Anti-Virus Emergency Response Team), contacting, 16

B

before you begin installation, 5
beta program, contacting, 16

C

Check Point, 12
command line
  installation properties, 37
  installing silently, 35
  installing specific features, 40
  installing the software, 33
  installing to a custom location, 35
  logging installation progress, 36
  modifying features, 52
  reinstalling and repairing files, 59
  removing the product, 65
  setting restart options, 41
  syntax, 34
contacting McAfee Security, 16
conventions used in this manual, 14
custom installation, 25
customer service, contacting, 16

D

DAT file
  updates, web site, 16
documentation for the product, 15
download web site, 16

E

EICAR test file, 46
ePolicy Orchestrator, 10

F

features, modifying, 48

G

getting information, 15

I

installation package, 10
installation package, pre-configuring with ePolicy Orchestrator, 10
installing VirusScan Enterprise
  before you begin, 5
  custom installation, 25
  preserving settings, 7
  system requirements, 8
  typical installation, 23
  using a login script, 41
  using the command line, 33
  using the Setup utility, 18
  where third party products are used, 11

K

KnowledgeBase search, 16

L

license, product, 13
login-script, installing the product, 41

M

manuals, 15
McAfee AutoUpdate Architect, 10
McAfee Installation Designer, 10
McAfee Security University, contacting, 16

N

Netopsystems' FEAD Optimizer, configuring, 67
network driver, loading, 25, 32

O

on-demand task, running after installation, 24, 31
operating systems supported, server and workstation, 8

P

pre-configuring the installation package
- using ePolicy Orchestrator, 10
- using McAfee AutoUpdate Architect and McAfee Installation Designer, 10

pre-installation recommendations, 6
preserved settings, 7
PrimeSupport, 16
processor requirements, server and workstation, 8
product documentation, 15
product overview, 5
product software, getting, 6
product training, contacting, 16
program files
- installing, 17
- modifying, 48
- reinstalling or repairing, 53
- removing, 61

R

RAM requirements, server and workstation, 8
reinstalling program files, 57
repairing program files, 57
restarting options via command line, 41

S

security headquarters, contacting AVERT, 16
service portal, PrimeSupport, 16
settings, preserved and not preserved, 7
Setup utility
- configuring the optimized file, 67
- installing the product, 18
- modifying features, 48
- removing the product, 61
- repairing files, 57

silent installation via command line, 35
submitting a sample virus, 16
system requirements, server and workstation, 8

T

technical support, 16
Terminal Services, 12
testing your installation, 46
training web site, 16
typical installation, 23

U

update task, running after installation, 24, 31
upgrade web site, 16
using this guide, 13

V

Virus Information Library, 16
virus, submitting a sample, 16